Propuesta Beatriz Galindo ENTEL/ISG

Área de Conocimiento: Ciencias de la Computación e Inteligencia Artificial

Universidad: Universitat Politècnica de Catalunya (UPC)

Departamento: Departamento de Ingeniería Telemática (ENTEL)

Antigüedad necesaria para el puesto: 7 años

Tipo de ayuda solicitada: Senior

1. PROYECTO DOCENTE

The teaching offer of UPC and, by extension, ENTEL, comprises several Masters' degrees. One of them is the "Master's degree in Cybersecurity", starting this next September 2020. The teaching project of this Beatriz Galindo proposal encompasses the context of such a Master's degree in Cybersecurity and aims at including a novel specialization on training and technical learning to protecting organization's critical infrastructures. The offer will uniquely explore, develop and operate data-driven methods, techniques and approaches to detect, analyze and mitigate debilitating cyber-threats. The program's actionable outcomes will be distributed to public, private and academic entities by instrumenting innovative and operational cyber security capabilities. A brief outline of the initial planning follows.

Master's degree in Cybersecurity.
Specialization on cyber-resilient techniques to protect organization's critical infrastructures

1. Objectives

- Prepare students to:
  - Architecture and integrate
  - Operate and maintain
  - Audit and expertise
- Targeting complex resilient systems:
  - Security and Dependability
  - Provide continuous service to users despite adverse conditions
  - Comply with regulations and best practices

- Compliance monitoring and evidence
- Domains:
  - IT and Telecommunications
  - Solutions vendors and integrators of Industry 4.0
  - Critical national infrastructures, owners and operators (energy, water, transportation)
  - Banking and finance sectors

2. Scope

2.1 Main Pillars

- Data resilience (Storage):
  - Privacy
  - Security
  - Persistency
- System resilience (Compute):
  - Virtualization
  - Malicious code
  - Monitoring, attack detection and mitigation
  - Fault tolerance
- Communications resilience (Network):
  - Virtual Private Networks (VPNs)
  - New networking technologies (SDN/NFV)
  - Monitoring, attack detection and mitigation
  - New protocols (SCADA, Supervisory Control and Data Acquisition)

2.2 Supporting methods, tools and new technologies

- Security
  - Identification and multi-factor authentication
  - Cryptographic protocols
- Dependability
  - Fault avoidance
  - Fault tolerance
- Standards and best practices
  - ISO27xxx
- Blockchain technologies
  - Integrity by design and scalability issues
  - Consensus mechanisms
  - Formal verification of security and privacy aspects
- Ways and means
  - Research and innovation: find the right tools to solve a given problem
  - Presentation skills: multi-level presentation of issues and solutions, from COMEX/CODIR to implementors/operators

3. Curriculum Organization

- Introduction to security and dependability (including practical hands-on refreshments on networking and system), **30h**

- Fundamental security techniques (models, authentication, property verification, etc.), **15h**
- Fundamental dependability techniques, **30h**
- Network security and dependability, **30h**
- Systems and virtualization, **45h**
- Information security and privacy, **30h**
- Industrial control systems, **30h**
- Legal and economic aspects, **15h**
- Bibliographic in-depth security or dependability project, **45h** ***(homework)***
- Final project (two students, in relation with industry), **225h** ***(homework)***

As an example, we elaborate next on a sample graduate course on "**Industrial Control Systems (ICS)**" considering real-world problems in ICS posed by external stakeholders (e.g., industrial partners collaborating with ENTEL/ISG, such as system-owners and related ICS experts). The requirements of the new course are being innovative and incorporating the latest advances in recent scientific fields on the topic. The approach of the course, as well as its format and expected outcomes of the associated modules, follows.

Graduate course on "Industrial Control Systems (ICS)", MSc on Cyber-Resilience
Semester I, 6 ECTS, Compulsory

1. Approach

The pedagogical approach of this course consists on *learning by doing*. It assumes students working in small groups, collaborating in order to solve real-world problems, leveraging on prior courses and training, and using their own knowledge, skills and abilities. Existing examples from the attached bibliography will be put in practice. More specifically, active teaching examples reported in the cyber-physical education community, building upon curricula that addresses the needs to train learners and professionals on critical infrastructure protection and resilience of industrial control systems. Teaching will be complemented with interactive laboratories and hands-on training. For example, live exercises demonstrating current vulnerabilities associated with commercial SCADA (*Supervisory Control and Data Acquisition*) industrial products will

be implemented with fully packaged Linux-based computer science lab exercises based on existing software at https://my.nps.edu/web/c3o/labtainers.

2. Requirements

Prior to enrolling to the course, students will be assumed to have completed basic courses on computer and network protection technologies (from a functional standpoint). It is also expected that the students would have experience on the use of virtualisation techniques (e.g., installation of virtual machines, discovery of software vulnerabilities) as well as deployment of countermeasures, use of penetration testing tools and reasoning about misuse of ICT systems from an adversarial perspective. Such knowledge will be provided and evaluated in the initial (introductory) courses of the main MSc program. Then, the course will start with some introductory modules, on ICS fundamentals (covering topics such as *Networked Control Systems*, *Distributed Control Systems, SCADA Technologies*, *Human Machine Interfaces*, *Programmable Logic Controllers*, etc.) and industrial protocols (such as Modbus, DNP3, PROFINET, etc.). In the end, the students will learn from these introductory modules the main similarities and dissimilarities between traditional ICT protection vs. protection of industrial control systems. The introductory modules will be complemented with homework assignments and practical laboratories.

3. Assignments

Homework assignments will consist of assigned readings, including both technical and scientific paper readings, white papers, and probably background materials and video recordings on ICS security research provided by the industrial partners collaborating in the proposed programme. Such reading assignments shall be followed by written reports provided by the students, in which they shall provide a short-written synopsis, including a constructive evaluation and discussion on the pros and cons of the topics covered by the provided materials. Practical laboratories will be provided to the students on topics such as vulnerabilities and management of countermeasures. The laboratories will leverage on the experimental platforms and testbeds described in the research programme, as well as potentially some SCADA-in-a-box lab

environments (e.g., https://www.tofinosecurity.com/ and https://www.hns-platform.com/ products). In the end, students will directly interact with common ICS components, including aforementioned PLCs, HMI software, SCADA firewalls, and SCADA IDSs. Laboratory exercises and *learning by doing* activities, such as *capture the flag* and *wargames*, will be conducted. In such exercises and activities, student teams will be requested to conduct attacks on some of the unprotected SCADA components (e.g., unprotected PLCs) by misusing them from an adversarial perspective, while the remainder team of students will be requested to configure countermeasures, such as activation of SCADA firewall rules, reconfiguration of routers to divert SCADA protocol traffic (e.g., ModBus traffic between HMIs and PLCs) to monitoring or disinfection services.

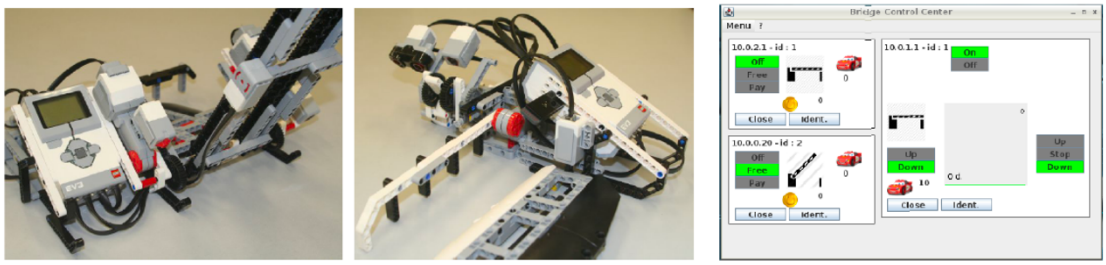
4. Sample Platform

Some practical activities associated to the training in this course will be conducted using some testbed environments for working on attack and defense of hybrid cyber-physical attacks, targeting cross-layer protocols for the control of industrial networks. This includes the ability to study attacks triggered either at lower or upper layers, and affecting both centralized and decentralized infrastructures. It leverages upon current work already started to adapt pedagogical platforms like Lego Mindstorms and Raspberry Pi, to study the security of industrial control system protocols like PROFINET, DNP3 and Modbus; as well as their interaction with carrier networks and SDN (Software Defined Network) technologies.

Given the difficulty of handling threats at the upper layers of industrial network technologies, some assessment techniques will be tested directly at the lower layers (e.g., sensors and local units). For instance, adaptation of physical-layer failure detection mechanisms (e.g., systems for the detection of faults and accidents) to handle, as well, malicious actions (e.g., integrity attacks conducted by malicious entities). The goal is to further elaborate on such approaches, handle current limitations, and explore new innovative cross-layers solutions beyond the state of the art. The underlying framework leverages from control and configuration theory algorithms covering both faults, accidents and also attacks, with the aim of managing the protection of industrial protocols as a whole.

The use of co-simulation will allow us to experiment with attacks and mitigation actions, as well as to validate theoretical and simulated solutions with real-world devices. The goal is to analyze the limitations of state-of-the-art countermeasures in network and physical control processes.

Figure 1 depicts a co-simulation to represent data integrity attacks against the SCADA controller of a weighing bridge system. Figure 1(a) shows some Lego Mindstorms EV3 components used as Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs) of the SCADA scenario. Figure 1(b) shows a Human Machine Interface (HMI) at the control center. Together, they allow us to implement experimental RTU and PLC automata, developed using the same software and hardware libraries. Under normal conditions, the HMI at the control side sends commands to control the RTUs. Likewise, the RTUs send some commands to the specific PLCs, to instruct the actuators or to request data from the sensors. A sample attack scenario using the proposed setup would work as follows. The HMI requests to the system to get down the bridge. Right after the bridge starts getting down, and the control center HMI depicts the bridge as closed, an attacker eavesdrops the exchange of messages (exchanged over Modbus/TCP) and gets control of the system by conducting the integrity attack. In the end, the co-simulation platform helps at showing and validating that having network and physical protection separated fails at protecting the SCADA system.



(a) Bridge and Toll (*Lego Mindstorms EV3*) (b) Human Machine Interface

Figure 1: Lego Mindstorms EV3 co-simulation environment (cf. http://j.mp/TSPScada).

5. Outcomes

The set of modules, as well as their format and expected outcomes, rely on providing a realistic hands-on experience to the students, in order to enhance their know-how on computer and network functional protection, with additional knowledge and real-world practice on operational aspects of SCADA and further ICS technologies. Once all the activities will be concluded, the

student teams will be requested to derive further countermeasures and mitigation solutions, and publicly communicate their proposals in seminar-like sessions. Experts and stakeholders will be invited as part of the jury panels that will evaluate students' results. Such results will be evaluated in terms of critical thinking and novelty of the solutions. Students will also be requested to develop short reports explaining their understanding of the activities, focusing on the precise components provided to them in each environment, as well as the protection mechanisms, problems encountered during the laboratory activities and the way in which the problems were solved by each team.

Bibliography

T. Nguyen, M. Gondree, "Teaching industrial control system security using collaborative projects," in Security of Industrial Control Systems and Cyber Physical Systems. Springer, 2015.

J. Foreman, J. Graham, J. Hieb, and R. Ragade, "A curriculum model for industrial control systems cybersecurity with sample modules," in Technical Report 2012-14, Center for Education and Research, Purdue University. Purdue University, 2012.

S. Mishra, T. Howles, R. Raj, C. Romanowski, J. Schneider, A. McNett, "A modular approach to teaching critical infrastructure protection concepts to engineering, technology and computing students," in Frontiers in Education Conference. IEEE, 2016.

R. Vaughn, T. Morris, and E. Sitnikova, "Development & expansion of an industrial control system security laboratory and an international research collaboration," in Eighth Annual Cyber Security and Information Intelligence Research Workshop. ACM, 2013.

M. E. Luallen and J.-P. Labruyere, "Developing a critical infrastructure and control systems cybersecurity curriculum," in System Sciences (HICSS), 2013 46th Hawaii International Conference on. IEEE, 2013.

S. Weerakkody, O. Ozel, Y. Mo, B. Sinopoli. Resilient control in cyber-physical systems: Countering uncertainty, constraints, and adversarial behavior. Foundations and Trends R in Systems and Control, 7(1-2):1–252, 2020.

R.W. McGrew and R. B. Vaughn, "Discovering vulnerabilities in control system human–machine interface software," Journal of Systems and Software, vol. 82, no. 4, pp. 583–589, 2009.

2. PROYECTO INVESTIGADOR

Industries, governments, and individuals have embraced the many advantages that the cyberspace offers to the benefit of our economy and life quality. However, our dependence on cyberspace makes us very vulnerable to attacks. This includes threats related to national security and economic growth. The cyberspace can debilitate and disrupt digital infrastructures at very high speed and in full anonymity. A large number of European companies have been the targets of cyber-attacks, with more than 80% of them enduring a significant financial loss [R1]. The problem is drawing a great deal of attention since 2010, the year in which the infamous Stuxnet incident uncovered a successful cyber-physical sabotage of a uranium enrichment plant in Iran [R2, R3]. Similar incidents include disruption of financial services [R4, R5], as well as hacking of autonomous cars and aviation systems [R6, R7].

Public safety is also affected by cyber-incidents [R5], increasing even more the number of critical infrastructures in which a single successful attack could cause not only monetary loss, but also impacts our way of life. Particularly attacks including Distributed Denial of Service (DDoS) activities severely threaten Internet and corporate networks [R8], while the recent trend of ransomware continues to target a plethora of victims from various sectors, also causing significant financial loss damages [R9]. The aforementioned issues are particularly relevant with the emergence of pervasive paradigms, including the Internet of Things (IoT) and Industrial IoT (IIoT). These paradigms benefit from innovations in computing power, electronics miniaturization, and extended network interoperability, leading remote embedded sensor devices towards environments that automate the generation, exchange, and processing of data with minimal human intervention. The impact to our lives of both IoT and IIoT is expected to be quite disruptive, with a myriad of technological industries and enterprises building upon billions of

connected sensing devices, and transforming our economies [R17]. The proper deployment of such technologies promises indisputable benefits in manufacturing plants, power utilities, and building automation. Nevertheless, the scarcity of proper legislation, as well as cost and time-to-market considerations, heads to potentially insecure devices. Such devices can quickly be recruited into malicious botnets [R18], hindering insecurity widespread in various sectors and critical infrastructures, including next-generation cyber-physical systems [R19].

Research program: Cyber Threat Intelligence for Resilient Systems is an open problem identified by major research communities and working groups such as the IEEE Computer Society Technical Committee on Security and Privacy [R10, R11], the IEEE Control Systems Society [R12, R13], as well as by European and American research agencies [R14, R15, R16]. Challenges include: (1) the design of novel approaches to protect systems that enable integration of control, communication, and computation, compounded by uncertainty and unreliable environments affected by malfunctions and intentional (human-level) attacks; and (2) foundational science for seamless protection and resilience of complex technologies that are embedded in autonomous cyber-physical systems, satisfying critical constraints such as safety, security, privacy and performance.

In the long-term, the vision of the proposed research program is to conduct large-scale cyber security research, development, operations, training, and dissemination activities. The goal is to explore and investigate innovative technologies and theories rooted in empirical Internet measurements for combatting evolving cyber threats, especially in domains including cyber-physical environments and critical infrastructures. The proposed research program is transformative in its capacity to design, implement, and evaluate novel and highly efficient algorithms, techniques, and methodologies that shall scrutinize raw, passive measurement cyber security big data to generate actionable and tailored cyber threat intelligence. Such intelligence will be exploited to infer, characterize, attribute, mitigate, and recover from contemporary cyber

threats. Further, the research program will innovate data-driven correlation engines between diverse cyber security empirical data to support the prompt investigation and attribution of cyber-attacks and their corresponding infrastructures. The research program will employ a unique, market-oriented approach in building and automating various operational cyber security capabilities to permit the distribution of the generated intelligence to European and international institutions, researchers, industry partners, data providers, and governmental entities.

The program's long-term scope also entails examining the practical and theoretical aspects of cyberspace to: (1) provide microscopic and macroscopic insights into the Internet's behaviour, usage, and evolution with special emphasis on its security aspects; (2) foster a collaborative environment in which empirical data and threat intelligence can be acquired, generated, analysed, and appropriately shared to enable impactful cyber security research and development; and (3) validate and advance the field of data science as it applies to cyber security and Internet measurements.

In the short term (i.e., within the following four years), the proposed research program will address the security and resilience of cyber-physical, IoT and IIoT paradigms in terms of property verification via formal methods. To this end, the proposed efforts will aim at proposing formal solutions for the construction of resilient designs since the conception phase. The programme will establish the foundations of a novel family of properties, and the construction of a general framework to allow automation engineers the development of advanced functionalities via formal specification of properties, refinement of models and synthesis of controllers. The objectives are summarized as follows:

- Objective 1: Enable the specification of cyber threat properties for resilient systems, including physical dynamics and adversary intentions, since the conception phase;

- **Objective 2:** Enable low-level refinement of cyber-physical and IIoT controllers, from high-level model abstractions, using automated synthesis-based tools, and providing the satisfiability semantics of the new properties;
- **Objective 3:** Enable the verification of properties at runtime, by cooperative cyber-physical and IIoT controllers, in a provable manner.

The experience, skills and methodological work to face the aforementioned challenges and objectives are the required guarantees for an appropriate transfer of knowledge to scientific communities and technological learners. To this end, the candidate who is expected to conduct the research program shall guarantee more than 10 years of imperative expertise related to operational cyber security, data analytics and cyber security for critical infrastructures. The expertise of the candidate should demonstrate a coherent alignment to the aforementioned research directions. The research program shall build upon the expertise acquired from previous contributions of the candidate as well as extend them to continually address evolving cyber intelligent threats, including those targeting cyber-physical and IIoT paradigms. The candidate shall leverage and encourage local and international research collaborations to address highly exploratory work and new research endeavours.

References

[R1] European Parliamentary Research Service, "Cybersecurity in the EU Common Security and Defence Policy (CSDP): Challenges and risks for the EU," 2017, Available Online: http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2017)603175

[R2] Falliere, Murchu, Chien, "W32.Stuxnet dossier, symantec security response," 2011, Available Online: http://j.mp/2jaM6uM

[R3] Langner, "Stuxnet: Dissecting a cyberwarfare weapon," Security & Privacy, IEEE, 9(3):49–51, 2011.

[R4] Greenberg, "The WannaCry Ransomware," 2017, Wired, http://j.mp/2CLdgkC

[R5] A. Greenberg. "Meet LockerGoga, the Ransomware Crippling Industrial Firms", 2019,

Wired. Available Online: http://j.mp/31ZoT2H,

[R6] Simmons, “Forget the Driverless Future. Get Ready to Physically Merge with a Car,” 2017, Wired, Available Online: http://j.mp/2yW61Dr

[R7] Biesecker, “Boeing 757 Testing Shows Airplanes Vulnerable to Hacking,” 2017, Aviation today, Available Online: http://j.mp/2B1RtrR

[R8] Sargent, Kristoff, Paxson, Allman, “On the potential abuse of IGMP”, ACM SIGCOMM, Computer Communication Review 47(1): 27-35 (2017).

[R9] Kharraz, Arshad, Mulliner, Robertson, Kirda, “UNVEIL: A large-scale, automated approach to detecting ransomware,” In USENIX Security Symposium, 2016, pp. 757-772.

[R10] Corman, Pillitteri, Tousley, Tehranipoor, Lindqvist, “NITRD Cyber-Physical Security Panel,” In 35th IEEE Symposium on Security and Privacy, IEEE S&P 2014, San Jose, CA, USA, May 18-21.

[R11] Yu, Fu, Song, Economides, Jo, Zhao (Eds), “Special Issue on Security and Privacy in Cyber-Physical Systems,” In IEEE Internet of Things Journal, volume 4(6), December, 2017.

[R12] Baheti and Gill, “The impact of control technology – cross-cutting research directions,” In IEEE Control Systems Magazine, pages 161–166, 2011.

[R13] Sandberg, Amin, Johansson, “Cyberphysical security in networked control systems,” In IEEE Control Systems, 35(1):20–23, 2015.

[R14] National Science Foundation, “Cyber-Physical Systems (CPS), Program Solicitation no. 17-529,” 2017, Available Online: https://www.nsf.gov/pubs/2017/nsf17529/nsf17529.htm

[R15] S. Weerakkody, O. Ozel, Y. Mo, B. Sinopoli. Resilient control in cyber-physical systems. Foundations and Trends R in Systems and Control, 7(1-2):1–252, 2020.

[R16] European Commission, “Seamless authentication for all,” 2018-2020, Crack the challenge. Available Online: http://ec.europa.eu/research/horizonprize/index.cfm?prize=authentication

[R17] Cisco Systems, “Global Impact of the Internet of Things,” Available Online: https://www.cisco.com/assets/sol/dc/global_impact_of_internet_of_things.pdf

[R18] Bertino and Islam, “Botnets and Internet of things security,” 2017, Computer 50(2): 76-79.

[R19] M. Barbeau, G. Carle, J. Garcia-Alfaro, V. Torra. "Next Generation Resilient Cyber-Physical Systems", arXiv:1907.08849, Available Online: https://arxiv.org/pdf/1907.08849

3. TRANSFERENCIA DEL CONOCIMIENTO A REALIZAR

Cyber-attacks are not games played by computer geeks anymore. They suppose serious crimes, which can disrupt and bring down critical infrastructures, e.g., affecting nation states on Industrial Control Systems (ICSs), like those that look after public services – telecommunications, water and waste control, energy and transportation. Cyber-attacks are not only increasingly common, they are a threat to society and to our individual safety.

According to current global information security study in 2019, the global cybersecurity-workforce shortage will reach upwards of 1.8 million unfilled positions in the next ten years. In a similar line, Julian King, the EU's Commissioner for Security Union, recently stated that "Europe faces a cyber-security skills gap, a shortfall currently estimated to sum to 350,000 people by 2022". In response to this worrying situation, this proposal aims at creating and providing the knowledge gap to train the future leaders of cyber-security team of public sectors and large companies, as well as in start-ups and SMEs. The proposal aims to address this challenge by properly guaranteeing the training and educating cyber-security learners to leading to problems in the realm of cyber-resilience. This differs from traditional training mainly focused on cyber-protection (e.g., cryptography, access control, anonymity, watermarking) and cyber-defense (e.g., intrusion detection, mitigation, correlation of alerts, supervisory events systems), two disciplines which are still important, but that are not sufficient to handle the problem anymore.

The teaching and research project associated to this proposal will foster the transfer of competitive and innovative knowledge needed by new learners and early researchers to design new solutions that require the assumption of security beyond breach. The transfer of knowledge in terms of attack-tolerance techniques tailored to systems that have a direct impact on the physical

world, is in tune with societal needs. Agencies such as ENISA (the EU Agency for Network and Information Security) keep alerting about the worryingly low level of maturity of practical solutions with a structured approach to develop resilient infrastructures evolved from our conventional technology. The transfer of knowledge from the proposal is also expected at the level of employability, assuring tutoring and guidance of people in crucial sectors needing from new ways of dealing with the challenges of today and tomorrow.

4. IMPACTO DESEADO EN LA UNIVERSIDAD

With the incorporation of the senior candidate of the Beatriz Galindo program, UPC intends to increase the scientific impact of new research lines, as well as give continuity to an existing project of regeneration of teaching and research faculty members. More specifically, the impact expected from the recruitment of the candidate include, but is not limited, to:

- Publications in international journals of maximum impact.
- Representation in international conferences of first level.
- Training of students on security, privacy and resilience topics at the highest level.
- Release of open-source software and hardware, testbeds and platforms, for both academic and industrial ventures.
- Promotion of industrial and pedagogical chairs with industry.

Fundamental theoretical advances in information security, privacy, and resilient automation methods constitute other important impacts. The value of such outcomes shall impact the economics of automation, advancing risk-averse industries, especially those related to academic and industrial partners of UPC in related areas. Such outcomes will also be explored to promote the creation of an international research lab, in a similar way as the EU Joint Research Centres on

cybersecurity like EPIC or CIIP (cf. https://ec.europa.eu/jrc/en/research-topic/cybersecurity), succeeded in establishing consolidated products that are now used in industry.

Impact shall meet as well the needs expressed by the European Factories of the Future Research Association (EFFRA), the European Cyber Security Organization (ECSO), and the ICT-03 SPARTA network of excellence in terms of cyber-security training. The national and economic security of the European countries strongly depends on the reliable functioning of their infrastructures and technology adopted in such systems. There is a need of new experts and the projects undertaken by the candidate shall contribute to maximize employability of those experts trained with the new skills and outcomes of both the teaching and research projects of this proposal, to become key academic or industrial leaders, at the forefront of advanced technologies for the security of industrial critical systems. Social impact, boosting competitiveness with the aforementioned outcomes, with an open transfer of the proposed solutions transversely to industrial partners, including large, medium, small enterprises, as well as creation of new spin-off ventures (including career perspectives and employability of young researchers contributing to the candidate project, e.g., PhD students and postdoctoral fellows).

Finally, the expected transformational impact in science, technology and society includes as well technological changes in digital security for cyberspace. Such changes need to be developed with scientific rigor to achieve sustainability and scalability, to strike the right balance between transparency and privacy, and to find the right mix between decentralization and accountability to governance bodies. The programs associated to the senior candidate of this Beatriz Galindo proposal (in terms of teaching, training and research) contribute to crucial designs for digital security and resilience of cyberspace technologies, which are the challenges driving the senior candidate of the proposal.

5. EMPLEABILIDAD DEL CANDIDATO

The teaching and research profile of the candidate comes from the cyber-security area, in line with the needs and expertise of the ENTEL Department of UPC (Departamento de Ingeniería Telemática, Universitat Politècnica de Catalunya), with a very successful international impact in this field of extraordinary research. The proposed candidate will allow ENTEL to expanding said international status, and continue with the relevance achieved during these last years.

ENTEL includes 54 professors who teach within the scope of telematics engineering at four centres: ETSETB, EETAC, EPSEVG and ESEIAAT. Moreover, ENTEL is responsible for the Master and Ph.D. programs in Telematics Engineering. The research activities in the Department mainly focus on Telematics Services, Design and Evaluation of Networks and Broadband Services, Wireless Communications, and Management, Policy and Services Prices in New Generation Networks. Furthermore it has carried out numerous research projects and technology transfers, both nationally and internationally, with public and private funding.

The incorporation of the candidate within ENTEL is backed by the ISG research group, under the scope of their "Security and Privacy" program.

The ISG group was created in 2002 by Full Professor Miquel Soriano, and a group of young network engineers making their first steps as faculty. From the very beginning, the main strategic objective of the ISG group was to be the reference security group at UPC, and all members of the group joined forces towards this goal. Now, after 15 years of working together, the results obtained are self-explanatory:

- 163 papers in ranked journals.
- 321 papers in conferences.
- 60 competitive projects.

- 20 read thesis and 17 books and book chapters.
- 12 awards.
- 9 patents.
- 14 six year period of research activity, 7 of the 9 professors have it on going ("sexenio vivo").

The group has obtained the GRC mention in all the previous calls (all of them with funding):

- In 2005 call, SGR- 01015 (37.600 euros).
- In 2009 call, 2009-SGR-1362 (71.760 euros).
- In 2014 call, 2014-SGR-1504 (30.000 euros).

New responsibilities of Professor Soriano (nowadays, vice-dean for teaching and research staff at UPC) have made him to delegate the leadership of the group to Professor Oscar Esparza, who is the only professor of the group that right now has the certification for full professorship by AQU (*Agència per a la Qualitat del Sistema Universitari de Catalunya*). Prof. Esparza has advised three doctoral theses, co-authored 30 articles in ISI-JCR indexed journals and almost 40 papers in conference proceedings. He is member of the TPCs of many international conferences, and editor of the Wireless Communications and Mobile Computing journal. The core of the ISG group is formed by 1 full professor, 7 associate professors (3 "professors titulars" and 4 "professors agregats") and 1 assistant professor ("col·laborador doctor"). These members have a wide knowledge in the area of network security, and currently perform their research activities in topics like blockchain, IoT security and privacy, digital forensics, network coding and security protocols.

The ISG group has a very coherent scientific strategy when dealing with different aspects of cyber-security research, in which the proposal of the candidate nicely fits to expand they cyber-security expertise with novel research scenarios including protection beyond adversarial breach.

The group has a clearly recognized international position, which not only appears in its publications, but also through its participation in executive committees of international societies in the security field and their participation in the editorial boards of leading scientific journals.

Both ENTEL and ISG will provide all possible facilities for the integration of the candidate, properly tailored to the projection and performance of the candidate during the enjoyment of the Beatriz Galindo aid. UPC has already put in place all the necessary mechanisms to assure that the selected candidate will opt for a permanent position in the institution. The support that will be given by UPC to the incorporation of the senior candidate of the Beatriz Galindo aid is also part of UPC policies to attract new talent. The commitment of ENTEL and ISG to this objective is based on the actions taken by UPC in the last five years

As regards to the specific support to be given to the candidate if elected, ENTEL and ISG count with all necessary resources relating to (1) human resources (e.g., research members, PhD students, technicians, postdoctoral fellows); (2) material resources (e.g., lab space, equipment, cluster of computers, and communications equipment); and (3) financial resources (e.g., involvement in international and national-level projects).

The integration process of the candidate will be carried out in two phases: (1) knowledge adaptation process, in which the candidate will consolidate his involvement with the needs of both ENTEL/ISG and other existing research groups at UPC, by properly establishing synergies and helping to consolidate existing lines and/or promote new research lines based on the Beatriz Galindo project; and (2) incorporation process, in which ENTEL and ISG will conduct the process of integration of the candidate, by assessing the effectiveness of the employability of the candidate and allocating all the required funds for his permanent position.